UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/710,310	07/01/2004	David S. Bonalle	70655.1600	4309

20322 7590 04/05/2006

SNELL & WILMER
ONE ARIZONA CENTER
400 EAST VAN BUREN
PHOENIX, AZ 850040001

EXAMINER	
HESS, DANIEL A	
ART UNIT	PAPER NUMBER
2876	

DATE MAILED: 04/05/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	**Application No.** 10/710,310	**Applicant(s)** BONALLE ET AL.	
	Examiner Daniel A. Hess	**Art Unit** 2876	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *18 January 2006*.

2a)□ This action is **FINAL**. 2b)☒ This action is non-final.

3)□ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-10,12,15-27,29-42 and 44-52* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)□ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-10,12,15-27,29-42 and 44-52* is/are rejected.

7)□ Claim(s) _____ is/are objected to.

8)□ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)□ The specification is objected to by the Examiner.

10)□ The drawing(s) filed on _____ is/are: a)□ accepted or b)□ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)□ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)□ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)□ All b)□ Some * c)□ None of:

1.□ Certified copies of the priority documents have been received.

2.□ Certified copies of the priority documents have been received in Application No. _____.

3.□ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) □ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) □ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date _____.

4) □ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ .

5) □ Notice of Informal Patent Application (PTO-152)

6) □ Other: _____.

DETAILED ACTION

This action is in response to 1/18/2006 amendment and Request for Continuing Examination (RCE).

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

The text of those sections of Title 35, U.S. Code not included in this action can be found in a prior Office action.

Claims 1-8, 12, 15-27, 29, 30, 33-41 and 44-52 are rejected under 35 U.S.C. 103(a) as being unpatentable over Hoshino (US 6,636,620) in view of Maritzen et al. (US 2002/0191816).

Re claim 1: Firstly, Hoshino falls squarely within the realm of transaction systems. Although Hoshino's discussion of transaction systems, including such client-server systems as ATMs, is primarily in the background (columns 1 and 2 of specification; see especially column 1, lines 25-50), it is clearly conveyed that Hoshino's system is intended to be applied in the realm of such transaction systems. Hoshino discloses (column 4, lines 30-45):

> *"Each client terminal 30 includes a user input device in the form of a keyboard 42, an IC card reader 44, and a fingerprint sensor, preferably in the form of a semiconductor fingerprint sensor 46 (see FIG. 3). It also includes a*

> *communications section 62 for transmitting and receiving information to and from the server 32. The fingerprint sensor may sense information related to a fingerprint using a multiple of small capacitors to detect the ridges and valleys of a fingerprint. A client terminal user puts an IC card 48 into a slot of the IC card reader 44. Each IC card 48 stores personal information of the card owner. The stored personal information includes information related to an ID number of the card owner and information related to a fingerprint of the card owner. It is preferred that the fingerprint information be encrypted. "*

In the above description, the IC card is a smart card in communication with the reader. The reader is in communication with the biometric security system, for it performs the critical role of reading fingerprint data associated with an individual which is stored on the IC/smart card. The fingerprint sensor obviously detects a proffered fingerprint sample. Hoshino recites (column 4, lines 45 onward):

> *The client terminal 30 as illustrated in FIG. 2 carries an authenticator 64 in addition to the IC card reader 44 and the fingerprint sensor 46. The authenticator 64 is electrically connected to the finger print sensor 46 and the IC card reader 44. It compares information related to a sensed fingerprint with the stored fingerprint information on the IC card 48 and produces an authentication signal if the sensed fingerprint information matches the stored fingerprint information. A transmitter 50 is electrically connected to the IC card reader 44 and the fingerprint sensor 46 for transmitting the sensed*

> *fingerprint information, the personal information read by the IC card reader 44 and the authenticating signal to the server 32 only if the authenticating signal has been produced. A receiver 52, for receiving an authorization signal from the server 32, and a display 54, for indicating that a client terminal user has been approved for accessing the computer of the server 32, are preferably included in the client terminal 30. The keyboard 42 is used by the terminal user for entering information. The transmitter 50 is rendered responsive to the keyboard 42 for transmitting information entered by the keyboard 42 to the computer of the server 32 upon or after receipt of the authorizing signal from the server 32. A controller 56 controls operations of the client terminal 30.*

Thus, the device performs authentication using the sample and permits the transaction if a match is detected.

Lacking is an association of a particular fingerprint sample with a particular account.

Maritzen et al. teaches (see notably figure 6a and related description in the specification) that a fingerprint sample can be associated with an individual credit account. It is noted that credit accounts by their very nature usually have at least a maximum level transaction limit. That is certainly the case with Visa ™ shown in Maritzen, figure 6.

In view of Maritzen et al.'s teaching, it would have been obvious to one of ordinary skill in the art at the time the invention was made to include the old and well-known association of a fingerprint sample with a particular can because in this way a user can rapidly call up their account in a way that is resistant to fraud.

As for the newly added limitation, "fingerprint sample is primarily associated with a preset transaction limitation and secondarily associated with a user account and wherein said verification device is further configured to verify whether said proffered biometric sample is associated with said present transaction limitation and to verify compliance with said preset transaction limitation" the Examiner notes that since as Maritzen et al. shows a fingerprint sample associated with an individual credit account and since credit accounts can in turn normally have credit limits (certainly the case with Visa™ shown in Maritzen, figure 6), then by extension, it can be said that in Maritzen et al., fingerprints are by extension associated with transaction limits.

Re claim 2: In the case of Hoshino, the sensor performs authorization via communication, directly or indirectly, with a reader and a network (see figure 5). There are also dozens of known patents which teach a fingerprint sensor on the card itself.

Re claim 3: In the iteration shown in figure 4 of Hoshino, a finite number of scans is performed, namely one.

Re claim 4: (column 5, lines 50-55):

> If there is a match, the sensed fingerprint information by the fingerprint sensor 46 and the stored personal information read by the IC card reader 44 are transmitted from the terminal 30 to a server 32 long with an authenticating signal by step S6.

In order to send the sensed fingerprint data over a network, this data must be stored (logged) at least on a temporary basis.

As for a security feature being initiated, at least, access would be denied.

Re claim 5: From the abstract of Hoshino:

> "The database stores personal information of the service users. The stored personal information on the database includes information related to fingerprints and ID numbers of the service users. "

Re claim 6: In figure 5, the database is on a remote server.

Re claim 7: As discussed re claim 4 above, the server system, which is associated with the database, also receives the fingerprint sample.

Re claim 8: See column 4, lines 35-40: "The fingerprint sensor may sense information related to a fingerprint using a multiple of small capacitors to detect the ridges and valleys of a fingerprint."

These 'multiple small capacitors' are additional sensors.

Re claim 12: At a local level (see figure 2) an authenticator 64 performs comparison in Hoshino.

Re claim 16: As discussed above, the fingerprint information of Hoshino is associated with a user's account information. But in addition, the fingerprint information of Hoshino can also be associated with account information (such as a credit account) because it can be used for authorization related to such an account (see background). Note that this can be an indirect association: for example the fingerprint sample may be associated with a user who is in turn associated with a financial account. Thus the fingerprint is associated indirectly with the financial account.

Re claims 17 and 18: See figure 4 of Hoshino, the claimed arrangement is essentially shown.

Re claim 19: Hoshino does not have any teaching showing explicitly that notification is provided upon detection of a sample. However, the opposite, a failure of the reader to detect a sample, would be evident to the user simply by a lack of response to proffering a fingerprint sample. Positive notification is merely an equivalent. Further, the applicant has not shown that positive notification of sample detection would materially affect the workings of the invention, as compared with what can be considered passive notification.

Re claim 20: Financial transactions have already been discussed re claim 1 above.

Re claims 21, 34: The use of pin numbers is discussed in the background of Hoshino; using this as a secondary verification system would have been obvious, because two separate security measures provide greater security than just one.

As far as 'sending a signal to said host to notify…' it is understood that if access to the card is blocked due to lack of proper authentification, the host would be well aware of this, because the host is the entity through which authentication takes place.

Re claims 22-24: These limitations are taught in Hoshino; see notably discussion re claims 1-4 above.

Re claim 25: A capacitive scanner has been discussed re claim 8, above.

Re claim 26: Comparing the fingerprint sample with a stored version is at the center of Hoshino's verification system.

Re claim 27: See discussion re claim 6, above.

Re claim 29: See discussion re claim 12, above.

Re claim 30, 44: Hoshino discusses (column 6, line 37) ridges and valleys. These are minutia.

Re claims 33, 41: Repeating the security process with a second fingerprint sample can be described as a matter of repetition for the sake of added security such as to achieve a better match than could be achieved with just one sample. By analogy, police files typically include a *set* of fingerprints rather than just one, and thus achieve a better match than could be achieved with just one sample.

Re claim 35: See discussion re claim 1 above.

Re claim 36: See discussion re claim 2, above.

Re claim 37: See discussion re claim 8, above.

Re claim 38: See discussion re claim 4, above.

Re claim 39: See discussion re claim 3, above.

Re claim 40: See discussion re claim 4, above.

Re claim 45: See discussion re claim 5, above.

Re claim 46: See discussion re claim 12, above.

Re claim 47: See discussion re claim 12, above.

Re claim 48: Hoshino discloses (column 4, line 45):

"It is preferred that the fingerprint information be encrypted. "

Re claim 49: As discussed re claim 48, encryption is employed in Hoshino. The use of public and private key encryption is an extension of this, a common example of an encryption scheme regarded as secure.

Re claims 50-52: As per the discussion re claim 1 above, it is the nature of credit accounts that there is usually at least a maximum level transaction limit. That is certainly the case with Visa ™ shown in Maritzen, figure 6.

Claims 9 and 31 are rejected under 35 U.S.C. 103(a) as being unpatentable over Hoshino / Maritzen as applied to claim 1 above, in view of Kamei (US 5,901,239).

Hoshino discusses (column 4, line 37) ridges.

Lacking is a specific teaching of the specific types of minutiae compared.

Kamei teaches in a fingerprint analysis system, differentiating among specific minutiae including (column 7, lines 55+), ridge ends, valley bifurcations...

In view of Kamei's teaching, it would have been obvious to one of ordinary skill in the art at the time the invention was made to include differentiation among the old and well-known minutiae of a fingerprint such as ridge ends, valley bifurcations etc. because this can provide more accurate identification. These features are generally common among detected fingerprints and the motive for testing a variety of features is to have more data with which to perform verification.

Claims 10, 32 and 42 are rejected under 35 U.S.C. 103(a) as being unpatentable over Hoshino / Maritzen as applied to claim 1 above, in view of Tuli (US 5,942,761).

Hoshino / Maritzen fails to teach specific measurement of those non-fingerprint variables recited.

Tuli teaches (column 3, lines 44+) detection of body heat in association with fingerprints.

In view of Tuli's teaching, it would have been obvious to one of ordinary skill in the art at the time the invention was made to associate detection of body heat with fingerprint authentication in order to verify that the sample is indeed coming from a live finger as opposed to, for example, a finger formed from a mold.

Response to Arguments / Amendment

Applicant's arguments filed 1/18/2006 have been fully considered but they are not persuasive. In particular, the Applicant has taken the position that the newly added limitation,

"fingerprint sample is primarily associated with a preset transaction limitation and secondarily associated with a user account and wherein said verification device is further configured to verify whether said proffered biometric sample is associated with said present transaction limitation and to verify compliance with said preset transaction limitation"

The Examiner notes that Maritzen et al. (of record) teaches (see notably figure 6a and related description in the specification) that a fingerprint sample can be associated with an individual account. Accounts in turn are typically associated with a transaction limit.

Therefore, by extension, it can be said that in Maritzen et al., fingerprints are **by extension** associated with transaction limits.

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Daniel A. Hess whose telephone number is (571) 272-2392. The examiner can normally be reached on 8:00 AM - 5:00 PM M-F.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Michael G. Lee can be reached on (571) 272-2398. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Daniel A Hess
Examiner
Art Unit 2876

3/24/06